ORDER FOR SUPPLIES OR SERVICES (FINAL)

PAGE 1 OF 1

N65236-13-D-4956	0003	2015 Dec 23	N65236-15-NR-55279	Unrated

6. ISSUED BY CODE N65236 SPAWAR-Systems Center Lant (CHRL) P.O. BOX 190022 North Charleston SC 29419-9022 Melissa A Connell/2.2.53 843-218-2701	7. ADMINISTERED BY CODE S2101A DCMA Baltimore 217 EAST REDWOOD STREET, SUITE 1800 BALTIMORE MD 21202-5299	8. DELIVERY FOB □ DESTINATION □ OTHER (See Schedule if other)
9. CONTRACTOR CODE 15151 FACILITY HONEYWELL TECHNOLOGY SOLUTIONS 7000 COLUMBIA GATEWAY DRIVE COLUMBIA MD 21046	10. DELIVER TO FOB POINT BY (Date) See Schedule 12. DISCOUNT TERMS Net 30 Days WIDE AREA WORK FLOW 13. MAIL INVOICES TO THE ADDRESS IN BLOCK See Section G	11. X IF BUSINESS IS □ SMALL □ SMALL DISADVANTAGED □ WOMEN-OWNED
14. SHIP TO CODE See Section D	15. PAYMENT WILL BE MADE BY CODE HQ0338 DFAS Columbus Center,South Entitlement Operations P.O. Box 182264 Columbus OH 43218-2264	MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER	DELIVERY/ CALL	X	This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of numbered contract.
	PURCHASE		Reference your furnish the following on terms specified herein.
			ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

HONEYWELL TECHNOLOGY SOLUTIONS		Jerry Erar Principle Contracts Manager	
NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMDD)

□ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE

See Schedule

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED *	21. UNIT	22. UNIT PRICE	23. AMOUNT
	See Schedule				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.	24. UNITED STATES OF AMERICA BY: /s/Carol A Lloyd 12/24/2015 CONTRACTING/ORDERING OFFICER	25. TOTAL	$11,389,044.55
		26. DIFFERENCES	

27a. QUANTITY IN COLUMN 20 HAS BEEN

□ INSPECTED □ RECEIVED □ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP NO. □ PARTIAL □ FINAL	29. D.O. VOUCHER NO.	30. INITIALS	
f. TELEPHONE / g. E-MAIL ADDRESS	31. PAYMENT □ COMPLETE □ PARTIAL □ FULL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR	
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.			34. CHECK NUMBER	
a. DATE / b. SIGNATURE AND TITLE OF CERTIFYING OFFICER			35. BILL OF LADING NO.	

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED	40. TOTAL CON-TAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

SECTION B SUPPLIES OR SERVICES AND PRICES

CLIN - SUPPLIES OR SERVICES

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
2001	J058	ICO Support Services - Funding #1 Integrated Cyber Operations Support Services in support of Integrated Cyber Operations (ICO) Portfolio mission areas in accordance with the contract PWS. Fixed fee will be applied to individual task orders in accordance with the offeror�s proposal in response to this solicitation. - CPFF (O&MN,N)	1.0	LO	(b)(4)		$11,389,044.55
200101	J058	ACRN: AA COST CODE: 000526ITQ14Q PLANNING PR #: 1300486765 FUNDED PR#: 1300539833 CRM #: 15-00757 Standard Doc. #: N6523615PR02941 Funding Doc #: N0005216RC001SC CIN 130053983300001 Network Activity #: 100001121462 0010 Funds Expiration: 9/30/2016 APPROPRIATION: 1761804 Type / Appropriation: Direct Cite (O&MN,N)					
3001	J058	ICO Support Services - Funding #1 Integrated Cyber Operations Support Services in support of Integrated Cyber Operations (ICO) Portfolio mission areas in accordance with the contract PWS. Fixed fee will be applied to individual task orders in accordance with the offeror?s proposal in response to this solicitation. - CPFF (O&MN,N) Option	1.0	LO	(b)(4)		$11,411,866.83
4001	J058	ICO Support Services - Funding #1 Integrated Cyber Operations Support Services in support of Integrated Cyber Operations (ICO) Portfolio mission areas in accordance with the contract PWS. Fixed fee will be applied to individual task orders in accordance with the offeror?s proposal in response to this solicitation. - CPFF (O&MN,N) Option	1.0	LO	(b)(4)		$11,588,396.04

SECTION C DESCRIPTIONS AND SPECIFICATIONS

TASK ORDER (TO) PERFORMANCE WORK STATEMENT (PWS)

SPACE AND NAVAL WARFARE SYSTEMS CENTER, ATLANTIC

SHORT TITLE: Commander, Navy Installations Command (CNIC) N6 Cybersecurity Support

1.0 PRIMARY PLACE(S) OF PERFORMANCE

The following sites are where the majority of labor hours will be spent; for travel (i.e., temporary duty sites) see Travel Section under TO PWS Para 10.0.

a. SPAWARSYSCEN Atlantic, Charleston facility
b. Contractor facilities – Charleston, SC

c. Government/Contractor Facilities, Washington D.C./National Capital Region

d. Government/Contractor Facilities, Hampton Roads, VA

e. Government/Contractor Facilities, Norfolk, VA

f. Government/Contractor Facilities, San Diego, CA

2.0 TASK ORDER PURPOSE

2.1 BACKGROUND

Navy ashore installations support our Navy's fleets, fighters and families. As the single responsible office, advocate and point of contact for Navy installations, Commander, Navy Installations Command (CNIC) has the mission to provide consistent effective and efficient shore installation services and support to sustain and improve current and future fleet readiness and mission execution. CNIC does this by providing unified and consistent procedures, standards of service, practices and funding to manage and oversee shore installation to the Fleet. CNIC executes delivery of installation services through its regions and installations. This mission involves the coordination of policy, planning, budgeting and reporting of all Navy regions and shore installations.

The mission of the CNIC Command Information Officer (CIO), Code N6, is to execute Department of Navy and Navy Chief Information Officer policies and programs and to provide Information

Management/Information Technology/Command & Control (IM/IT/C2) services required to support the mission of the Command. The CNIC N6 organization is tasked to provide an integrated framework of technology aimed at efficiently performing the business of CNIC. The CNIC N6 organization manages all aspects of the systems, and the supporting infrastructure, providing critical systems and infrastructure support enterprise wide.

2.2 SCOPE

SPAWARSYSCEN Atlantic currently provides technical and programmatic support to help CNIC with their mission to enable and enhance the combat power by providing the most effective, efficient, and cost-wise shore services and support. For this project SSC-LANT will provide Cybersecurity, Information Assurance (IA) and Information Security (IS) support to CNIC N6. Space and Naval Warfare Systems Center Atlantic (SSC-A) will execute engineering services to assist in ensuring compliance with Federal, Department of Defense (DoD), and Department of Navy (DON) and subservices regulations and policies. Navy IT performance is driven to maximum availability and efficiency through technically capable support teams with specialized knowledge, skills and experience supporting military applications and toolsets used by the United States Navy.

The objective of this Task Order is to assist SPAWAR in project execution, security operation support services, information assurance, certification and accreditation, Cybersecurity/IA policy, risk management services and network engineering services at locations throughout the Continental US (CONUS) and Outside the Continental US (OCONUS) areas.

3.0 APPLICABLE DOCUMENTS

3.1 REFERENCES

All references listed within the basic contract are required as applicable to this TO: In addition, the following reference(s) is identified specific to this TO:

	Document Number	Title
a.	NIST 800-66	Health Insurance Portability and Accountability Act (NIST 800-66, Resource Guide for Health Insurance Portability and Accountability Act of 1996 (HIPAA))
b.	NIST 800-53A	Federal Information Management Act (FISMA) of 2002 (NIST 800-53A, Guide for Assessing the Security Controls in Federal Information Systems)

c.	SECNAVINST 5239.3A	Secretary of Navy Instruction (SECNAVINST) 5239.3A, DON Information Assurance Policy
d.	DoDI 8500.1	Department of Defense Instruction (DoDI) 8500.1 Cybersecurity
e.	NIST SP-800-37	National Institute of Standards and Technology (NIST) SP-800-37 Guide for the Security Certification and Accreditation of Federal Information Systems
f.	NIST SP-800-53	NIST SP-800-53 Recommended Security Controls for Federal Information Systems
g.	DCID 6/3	DCID 6/3 Protecting Sensitive Compartmented Information Within Information Systems (DCID 6/3)—Manual
h.	Executive Order 12958	Executive Order 12958, National Security Information, Executive Office of the President, July 1995
i.	National Security Directive 42	National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, Executive Office of the President, July 1990
j.	Office of Management and Budget Circular A-130	Office of Management and Budget Circular A-130, Management of Federal Information Resources, Executive Office of the President, 8 February 96
k.	Public Law 100-235	Public Law 100-235, 101 STAT.1724, Computer Security Act of 1987, 8 January 1988
l.	NSTISS Policy No. 200	National Security Telecommunications and Information Systems Security (NSTISS) Policy No. 200, National Policy on Controlled Access Protection, National Security Telecommunications and Information Systems Security Committee, July 1987
m.	DITSCAP 5200.40	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) 5200.40, 7 October 1999
n.	DoDI 8510.bb	DoDI 8510.bb, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
o.	DoDI 8510.01	Risk Management Framework (RMF) Reissues and renames DoD Instruction (DoDI) 8510.01

p.	DoDI 8500.00	Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
q.	DoD 8570.01M	Department of Defense 8570.01 Manual – Information Assurance Workforce Improvement Program
r.	CJCSI 6510.01F	Information Assurance (IA) and support to Computer Network Defense (CND) 09 Feb 2011

3.2 SPECIFICATIONS

All specifications listed in the basic contract are applicable as required by this TO.

3.3 ACRONYMS

3.4 DEFINITIONS

4.0 SECURITY REQUIREMENTS

4.1 ORGANIZATION

As specified in clause 5252.204-9200 and the Contract Security Classification Specification form, DD-254, classified work shall be performed under this task order. The contractor shall have SECRET: at time of TO award OR prior to commencement of classified work a TOP SECRET with Sensitive Compartment Information (SCI) access facility security clearance (FCL).

4.2 PERSONNEL

Prior to commencement of work on this contract, all contractor personnel (including administrative and subcontractor personnel) shall have a favorable Trustworthiness Determination, which is determined by a National Agency Check with Local Agency Check and Credit Check (NACLC) and favorable FBI fingerprint checks. All personnel shall possess a SECRET clearance prior to working on TO. TOP SECRET with Sensitive Compartment Information (SCI) access facility security clearance (FCL) clearance may be required for various positions as specified in clause 5252.204-9200

5.0 COR DESIGNATION

The Contracting Officer Representative (COR) for this task order is (b)(6), *58100* who can be reached at phone **(843) 218-**(b)(6); e-mail: (b)(6)***@navy.mil***

6.0 DESCRIPTION OF WORK

The Contractor shall work closely with the CNIC System/Enclave (e.g., Service Delivery Point (SDP), Public Safety Network (PSNet), CINC Enterprise Support Center (CESC)) administration teams to provide cybersecurity support, such as troubleshooting of application issues, analyzing security event alerts and data, responding to incidents and problems, conducting root cause analysis and recommending improvements.

6.1. Cyber Security Operations

6.1.1. Command/Control Security Operation Center (C_2SOC)

The Contractor shall integrate capabilities within CNIC's IM/IT/C2 infrastructure to enable the C_2SOC staff to monitor, detect, scan, record, audit, analyze, investigate, report, remediate, coordinate, and track security-related "events" such as signs of intrusion, compromise, misuse, and compliance. The Contractor shall provide direct support to CNIC using government-furnished tools. The Contractor shall prepare templates and processes to produce trend analyses, scan reports, and vulnerability history.

6.1.2. Information Security Continuous Monitoring

The Contractor shall provide technical support for CNIC's Information Security Continuous Monitoring (ISCM) program and strategy. The CNIC ISCM program is based on the continuous monitoring process described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137.

The Contractor shall use the 3-tier risk management model defined in NIST SP 800-53 to support CNIC ISCM strategies,

At the organization (Tier 1) level to include:

- Create a framework to support the Office of Management and Budget (OMB) ISCM requirements,
- Centralize cybersecurity actions as an enterprise services for effective ISCM support of CNIC managed Information Systems (ISs),
- Support situational awareness by integrating asset awareness data with real-time vulnerability data,
- Incorporate real-time vulnerability data, operational data and IT knowledge base at the enterprise level to support informed IT decision, and
- Create enterprise methods and procedures to assign risk and to reduce maintenance and rework of ISs in order to mitigate risks;

At the mission/business process (Tier 2) level:

- Reduce CNIC IS risk posture and enable CNIC to operate within a known and defined risk tolerance with current vulnerability data and risk assessment, and

- Streamline System Development Lifecycle (SDLC) activities by automating tasks to support IS assessment and authorization; and

At the IS (Tier 3) level:

- Leverage existing and emerging cybersecurity systems and technology to fulfill ISCM requirements,
- Enable IS stakeholders to effectively manage IS in near real-time and respond to cybersecurity events and incidents as orderly and systematically as feasible.

6.1.3. 24x7x365 Cybersecurity Watch

The C_2SOC task covers the following areas: monitoring, detecting, scanning, recording, auditing, analyzing, reporting, remediation, coordinating, and tracking. All support described below shall be provided by the Contractor on a 24x7x365 basis.

6.1.4. Tier Cybersecurity Support

The cybersecurity watch, in conjunction with the CNIC Enterprise Support Center (CESC), shall respond as needed to assist with Tier I customer support with potential Cybersecurity related issues. The watch will follow initial incident response procedures in the C_2SOC Standard Operating Procedures (SOP) when an incident is identified. The watch may perform known and simple remediation actions if applicable. Complex cybersecurity issues shall be escalated by the watch to Tier II or Tier III and SPAWAR COR, per escalation processes defined in conjunction with the CESC.

6.1.5. Monitoring

The Contractor shall utilize CNIC provided sensors, systems, tools, and Government Furnished Equipment (GFE) to monitor all CNIC Networks and Systems for signs of intrusion, compromise, misuse, and non-compliance. The Contractor shall proactively monitor and track down anomalies, non-compliant systems, and other observed events that are detrimental to the overall security posture of CNIC IM/IT/C2 infrastructure and systems.

6.1.6. Detecting

The Contractor shall detect for vulnerabilities and sophisticated and nuanced attacks, discern and remove false positives, and analyze the information generated by CNIC Systems. The Contractor shall perform trend analysis to spot patterns within the CNIC network and depict representations of normal activities. The Contractor shall provide weekly and monthly reports. (CDRL A021) The weekly and monthly report shall be done via electronic mail only.

6.1.7. Vulnerability Scanning

The Contractor shall continuously scan the devices on the CNIC network to identify network and system vulnerabilities. The Contractor shall monitor the remediation status of the scan results and evaluate the scan results for accuracy and risk. The Contractor shall provide the analyzed results to the various responsible parties identified by the designated CNIC HQ N6 representative for resolution. The Contractor shall act as the Subject Matter Experts (SMEs) for the scan results and consult with the remediation teams on various methods for resolution. The Contractor shall produce and provide the following reporting deliverables and stated data elements:

Scanning report to include:

- Data and time of scan,
  - Network segment(s) scanned,
  - Individual who performed/verified scan,
  - Risk/threat level associated with scan, and
  - Roll up of scan results:
  - Network map with scan coverage
  - Network map with scanning results overlay
  - Pie chart that describes overall scan results;

Progress toward the continuous control in weekly and monthly reports (CDRL A021), which include:

- Internet Protocol (IP) Address ranges scanned,
- Numbers, categories and risks levels of vulnerabilities identified, and
- Remediation efforts being tracked;

Remediation report to include:

- Repeat findings,
- How long this vulnerability has been tracked and not remediated,
- Trending Information:
- Threat Level
- Sensitivity level of network segment; i.e. Computer Emergency Response Team (CERT) site
- How long the vulnerability has been identified but not corrected; and
- Mitigation suggestions.

6.1.8. Security Information and Event Management (SIEM)

The Contractor shall record, retain, and archive security event logs from various security systems on CNIC network using current deployed CNIC technology and equipment. The Contractor shall ensure all security event logs are synchronized with the Network Time Protocol (NTP) server for auditing, analysis and reporting. Logs shall also be maintained in accordance with current Department of Defense (DoD), Department of the Navy (DON), NIST and CNIC security policies to assist in event reconstruction and correlation. The Contractor is responsible for ensuring they are operating within the current DoD, DON, NIST and CNIC security policies. Security event logs shall include the following data:

- Source/destination IP address,
- Protocol/port number,
- Date and time with time zone,
- Event name,

- Event Priority/Level,
- Payload or flow data (Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)), and
- Session Duration.

6.1.9. Configuration Audit

The Contractor shall conduct weekly audits on the configuration of security event monitoring devices. The Contractor shall create a detailed plan for verifying the continuous monitoring, detection and response of security events on CNIC network. Weekly audits must include log reviews of successful and failed authentication attempts, file accesses, security policy changes, account changes (account creation, account deletion, and account privilege assignments), and use of privileges. The Contractor shall provide audit results in a weekly report for the devices listed.

The Contractor shall demonstrate, and report the status of, remediation efforts in weekly and monthly reports. (CDRL A021) These reports will incorporate various metrics as they are used in audit and other findings made available to and/or by the Contractor or designated SPAWAR LANT representative and other governing government entities.

6.1.10. Analysis (Log Review)

The Contractor shall act as a SME in daily log analysis for identifying security incidents, policy violations, and malicious code. Currently CNIC is using McAfee SIEM product suite for centralized audit log management. The Contractor shall use correlation engine to perform correlation of network IDS/IPS and Host Intrusion Prevention System (HIPS) logs with other records such as firewall/proxy logs, anti-virus, anti-malware, server audit trails as well as vulnerability information on CNIC targets. The Contractor shall conduct daily analysis of security logs to detect incidents on CNIC network and assist in remediation.

The Contractor shall create trend reports, to include the following, which will be submitted to SPAWAR on a weekly & monthly basis: (CDRL A021)

- Security events prioritize by Threat Level,
- Open & Close incidents,
- Black-listed or suspicious source IP targeting CNIC targets, and
- Forbidden or suspicious protocols and ports active on CNIC network.

6.1.11. Incident Response

If contacted by the CESC, the cybersecurity watch will provide Tier I cybersecurity support, open a log on the incident identified and perform known and simple remediation actions as applicable. Complex issues will be escalated by the watch and/or CESC for immediate actions.

6.1.12. Tier II Support

Contractor Tier II personnel shall be responsible for problem resolution and for investigating elevated issues by confirming the validity of the problem. Additional tasks that may be required of Tier II personnel would include: software repair, diagnostic testing, remote control tools, and replacing hardware components. Issues shall be escalated to Tier III or additional external support per C_2SOC SOP.

6.1.13. Tier III Support

The Contractor shall provide Tier III technical support that is comprised of senior level technicians who are responsible for handling the most difficult or advanced problems.

6.1.14. Coordination with External Resources

The Contractor shall coordinate with other DoD, DON and US Government agencies continually in order to provide information regarding security incidents that affect CNIC's IM/IT/C2 capabilities. Contractor shall use information from other agencies to improve the CNIC security posture and quickly react to fast moving threats directed by DoD, DON and/or the United States Computer Emergency Readiness Team (USCERT). The contractor may coordinate with external resources for further incident response support. External resources include engineering support from other external DoD resources (e.g., vendor, Original Equipment Manufacturer), as coordinated and/or approved by the SPAWAR LANT COR.

6.1.15. Remediation

The Contractor shall work with CNIC network administrators, program managers and system owners to oversee the remediation of identified security issues within CNIC's IM/IT/C2 capabilities. The Contractor shall oversee the resolution of security issues that may include:

- Installation of a software patch,
- Changes of a configuration setting, and
- Removal of the affected CNIC asset.

The Contractor shall provide a remediation plan that lists opened security issues with their steps and projected timelines for remediation. Remediation shall be tracked via the online portal mentioned in the previous section. The weekly report shall consist of an overview of security issues from the previous week and the status of each security issue including any outstanding issues, problems encountered, planned activities of interest for the next week and any lessons learned. The monthly report shall include only the outstanding issues, a summary of the action taken, problems encountered, responsible individual and milestones for resolution.

6.1.16. Incident and Service Tracking

Incidents, changes, and service requests are all currently controlled through the IPSwitch IssueTrak, ticketing system. The Contractor shall follow the C_2SOC SOP to manage incident ticket while making configuration changes, providing incident containment, eradication and recovery actions and engaging resources for incident response, such as gathering information. Incidents may identify underlying problems that require engineering work to fix design flaws or other issues. Work with SPAWAR LANT COR for infrastructure problems, this work shall be coordinated with other infrastructure support resources, such as enclave administrators, system owners and other contractors per designated CNIC HQ N6 representative.

6.1.17. Reporting (Daily and Monthly) Situation Reporting.

Contractor shall include in the monthly report of the number of incidents, changes, and service requests assigned in the reporting period. Continuous improvement is an objective for all processes, and the monthly report shall include all issues and recommendations to improve the process for future changes.

The Contractor shall provide daily and monthly situation reporting. The daily report shall cover each day's activities, the issues being tracked, and the status of each issue. The monthly report shall contain the following items:

- Duty roster,
- Summary of critical or urgent security issues being tracked,
- Status of each area of responsibility,
- Summary of critical or urgent administrative issues being tracked, and
- List of any needs/actions from the Government.

The Contractor shall provide a process to upload and maintain reports online – to a site to be specified by designated CNIC HQ N6 representative. The Contractor shall create a process to store watch logs and a watch supervisor turnovers.

6.1.18. Tools for Cybersecurity Management

- The Contractor shall be responsible for operating, tuning, and reviewing maintenance of all cybersecurity tools, software suites, devices, appliances and systems, including:
- The DoD Host Based Security System Suite (HBSS) suite, including the HBSS Enterprise Policy Orchestrator (ePO);
- The DoD Assured Compliance Assessment Solution suite;
- The McAfee SIEM product suite, including Enterprise Security Manager (ESM), Enterprise Log Manager (ELM), log receiver, event correlation engine or the equivalent replacements;
- ForeScout product suite, including CounterACT Enterprise Manager (CEM), CT appliances and plug-ins for Virtual Private Network (VPN) gateways;
- RedSeal cybersecurity configuration compliance appliances;
- WebInspect runtime web service cybersecurity monitors;
- Encase forensics management tool; and
- IDSs/IPSs:

o Continuous monitoring of the IDSs/IPSs for signs of compromise, misuse, compliance, and general health within CNIC networks,

o IDS/IPS operations:

§ Setup and deployment of IDS/IPS sensors

§ Provide recommended sensor policies

§ Tune sensor policies to reduce false positives

§ Provide specialized signatures

§ Tailor response events

§ Other day-to-day activities related to the IDSs/IPSs.

The contractor shall coordinate with CNIC network administrators, program managers and system owners (to include their contractors) to monitor activities and health of cybersecurity associated devices, such as Websense proxies, firewalls, and C_2SOC manageable routers, switches, agent servers and watch workstations.

6.1.19. Compliance Monitoring and Security Services

6.1.19.1. Operational and Technical Support for Security Services

The Contractor shall provide security services for protection of the ISs, IS domains (Communities of Interest), and Information Content (at rest, in use, and in transit) in accordance with DoD cybersecurity policies and procedures. These operational security services shall be fully integrated with the United States Cyber Command (USCYBERCOM) mandates to ensure confidentiality, integrity, availability, authentication, and non-repudiation requirements. The Contractor shall implement the necessary Information Assurance/Computer Network Defense (IA/CND) mechanisms to provide these security services, and conduct vulnerability assessments to validate that the necessary security controls (SCs) are in place. As part of implementing these security services, the Contractor shall implement CNIC directed IA/CND direction such as Information Operations Conditions (INFOCONs) and incident reporting (e.g., system anomalies, outages, etc.). Implementation of IA/CND mandates, to include USCYBERCOM Communications Tasking Orders (CTOs), Warning Orders (WARNORD), Operational Directive Messages (ODMs), Information Special Outage Report (INFOSPOT), Situational Awareness Report (SITREP), and Fragmentary Order (FRAGO) should be accomplished within Government specified timeframes as shown in Table 1 below.

Table 1 Compliance Timelines for Vulnerability Remediation

DoD Severity	NIST Severity	Days For Compliance/Approved Mitigation
Category (CAT) I	HIGH	Immediate – 25 Days
CAT II	MEDIUM	60 Days
CAT III	LOW	180 Days

CAT IV	INFORMATIONAL	

The Contractor shall provide strategic security services to enhance the confidentiality, integrity, and availability, authenticity, and non-repudiation requirements. The Contractor provided solutions shall support mechanisms of encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control. The Contractor shall provide informational feeds to support CNIC oversight, maintain accessible historical data, and deliver summary management reports that detail the security planning functions. The Contractor shall propose updated and/or revised architecture and/or configuration changes s to accommodate changing requirements, emerging technology, and results of vulnerability assessments for government review and approval.

6.1.20. Vulnerability Management

The Contractor shall meet the provisions of CNIC's Cybersecurity Vulnerability Management (IAVM) program implemented under Chairman of the Joint Chiefs of Staff Manual (JCSM) 6510.01A dated 24 June 2009 to include support for three types of vulnerability notifications:

- Cybersecurity Vulnerability Alert (IAVA) addresses vulnerabilities resulting in immediate and potentially severe threats to DoD systems and information. Corrective action is of the highest priority due to the severity of the vulnerability risk,
- Cybersecurity Vulnerability Bulletin (IAVB) addresses new vulnerabilities that do not pose an immediate risk to CNIC systems, but are significant enough that noncompliance with the corrective action could escalate the risk, and
- Technical Advisory (TA) addresses new vulnerabilities that are generally categorized as low risks to DoD systems.

The Contractor shall support the Vulnerability Management System issuances (IAVAs, IAVBs, and TAs); CNIC estimates a minimum of 25 monthly. The contractor shall meet the compliance timelines for IAVAs as issued and mandated by USCYBERCOM. The timeline for compliance on IAVBs and TAs vulnerabilities are determined by the assigned severity for the vulnerability coupled with the compliance timelines established by the Defense Information Systems Agency (DISA).

Severity codes ("Security Technical Implementation Guide (STIG) Finding Severity") are documented in the IAVM notices published on the USCYBERCOM Web Page. Table 2 below depicts the DISA compliance requirements based on severity. Such periods may be overridden by direction of the designated CNIC HQ N6 representative and communicated via a Plan of Action and Milestones (POA&M).Work with SPAWAR Government Team to ensure proper communication and direction.

Table 2 Compliance Timeline for IAVM Actions

DoD Severity	NIST Severity	Days for Compliance/Approved

		Mitigation
CAT I	HIGH	Immediate – 25 Days
CAT II	MEDIUM	60 Days
CAT II	LOW	180 Days
CAT IV	INFORMATIONAL	1000 Days

The Contractor shall take immediate action to assess the impacts of each vulnerability action, develop patching plans, and begin gathering data for the new "First Report" requirement. The patch plan should consider any other systems that may not be patched by POA&M report date.

In coordination with the network administrator, program manager, and/or system owner, the Contractor shall support the installation, configuration and testing of patches and changes required by Vulnerability Management System issuances (IAVAs, IAVBs, IAVMs) all necessary changes shall be made to the applicable production equipment in accordance with the suspense date articulated by the appropriate government authority. Patches or changes that require down time shall be coordinated with the designated CNIC HQ N6 representative in order to minimize downtime and/or schedule for non-peak time (e.g., nights, weekend). All patches or changes to the servers shall be performed on test servers prior to being applied to production.

The Contractor shall ensure IAVM compliance to include:

- The normal Certification and Accreditation (C&A) or Assessment and Authorization (A&A) process, and
- Monthly scanning of the systems using the most up-to-date version of the USCYBERCOM-approved vulnerability scanning package (currently, this is the Assured Compliance Assessment Solution (ACAS) Nessus Scanner by Tenable). The results of these scans will be sent to the appropriate system/network /enclave Information System Security Officers (ISSOs).

6.1.20.1. **Compliance to Connect**

The Contractor shall actively manage and integrate the ForeScout appliance suite with network routers, switches, firewalls and VPN gateways to provide cybersecurity compliance verification, enforcement and available remediation actions, when implemented, for network access control and secure remote computing.

6.1.20.2. **Network Equipment Configuration Compliance Monitoring**

The Contractor shall manage RedSeal appliances to continuously monitor cybersecurity compliance of configuration of CNIC network equipment and configuration change activities. Any network equipment configuration changes shall be reviewed to confirm that they are legitimate and authorized changes.

6.1.21. Maintenance of Standard Operating Procedures

The Contractor shall be responsible for maintaining the SOP of the C$_2$SOC, including:

- Adding new SOP items including new processes, procedures, forms, lists, etc. as they are introduced for C$_2$SOC operations,
- Updating existing SOP items to reflect changes and deletion of processes,

procedures, forms, lists, etc.,

- Maintaining the collection of the latest set of SOP items in the N6C-managed and designated shared portal, and

- Providing either hardcopy or online access of the latest set of SOP items to all C_2SOC watch station and watch analysts.

6.1.22. Cybersecurity Reporting

6.1.22.1. Daily C_2SOC Dashboard Update

Per designated CNIC HQ N6 representative review and approval, the Contractor shall implement a real-time dashboard reporting the status of key C_2SOC indicators by gathering data from CNIC's security services. The dashboard shall include:

- Key C_2SOC statistics such as number of outstanding incidents and estimated time to resolution, number of outstanding service requests

- List of top three outstanding incidents and estimated time to resolution

- List of top three outstanding service requests and estimated time to completion

- Operational status of all C_2SOC tools

6.1.22.2. Weekly Summary and Statistics

The Contractor shall collect weekly statistics, prepare and submit weekly summary to the SPAWAR LANT COR. Statistics and weekly summary will be delivered to the designated CNIC HQ N6 representative by noon of the first business workday of the following week. The weekly summary shall include:

- Breakdown of weekly hours expended by each category and/or key subcategory of the cybersecurity operations as discussed in Section 2 below,

- Present weekly hours expended by key subcategories in pie chart showing distribution of efforts,

- Present weekly hours expended by key subcategories in line chart showing trends in the last eight weeks, and

- Statistics of cybersecurity activities performed, including vulnerabilities scans; vulnerability management, including IAVA and IAVB; incident responses; completion of coordinating DoD mandates, including CTOs, WARNORDs, OTMs, Operational Orders (OPORDs) and FRAGOs.

6.1.22.3. DoD Reports

The Contractor shall assist CNIC in submitting required DoD cybersecurity reports, including:

- Online Compliance Reporting System (OCRS), and

- Continuous Monitoring and Risk Scoring System (CMRS).

6.2. Cyber Security Assessment and Authorization

6.2.1. Certification and Accreditation of CNIC's IM/IT/C2 Capabilities

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Provide assistance to system owner, enclave, or site personnel to complete required C&A documentation, addressing Independent Validation and Verification (IV&V) results and assisting enclave personnel in preparing Approval and Interim Approval to Operate (ATO) (IATO) for review by the Validator, Certifying Authority (CA), and the AO

- Review Security Design documentation to ensure comprehensive security requirements and compliance with DoD and Federal requirements and guidelines

- Review and provide input on physical, application and networking security polices procedures and practices

- Update CNIC N6 C&A Standard Operating Procedures (SOP) so that it aligns to DoD/DON policies

- Provide documentation support in the form of assisting with the writing and production of SOPs, Operational Manuals and review of government established and created Policies and Procedures as needed

- Support the implementation of Federal IT Security regulations, directives and guidance (Federal Information Security Management Act - FISMA, Federal Information Processing Standard - FIPS, National Institute of Standards and Technology - NIST series)

- Document the IA test plan and procedures templates for inclusion in the C&A Plan to appropriately relate the testing standard identified by the DAA/Navy Authorizing Official (NAO) and CA.

6.2.2. Support C&A Program Efforts with stakeholders

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Review updates of the DIACAP/Risk Management Framework (RMF) artifacts from the system owner and track status of changes

- Assist in the development of the path to complete accreditation

- Assemble the DIACAP/RMF Package, (DIACAP/RMF Scorecard, POA&M, Certification Documentation, and System-provided System Identification Profiles (SIPs) and DIACAP/RMF Implementation Plans) as appropriate

- Deliver the DIACAP/RMF Package to the CA in a trusted manner consistent with CNIC and/or Program requirements

- Provide C&A support in the areas of network topologies, file/application servers, encryption technologies, and network operating hardware and software

- Assess IA POA&M scheduling and completeness status and report
- Track assigned system from initiation to retirement, staying informed of IV&V milestones and DIACAP/RMF POA&M deadlines
- Address accreditation questions from the Program Management Office (PMO)
- Maintain accreditation schedules for systems. Work with the Program Management Office (PMO) to ensure the correct C&A process is being followed
- Adhere to certification guidance received from the CA and perform actions necessary to complete certification
- Participate in all test execution and planning activities, including meetings and working groups, as needed
- Participate in DIACAP/RMF Team Meetings and System review related meetings to provide technical and non-technical guidance,
- Identify and elevate the need for any additional IA test events needed to support accreditation (Includes scheduling of annual reviews)

6.2.3. Cybersecurity Validation Readiness Review

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Review and evaluation Self-Assessment results and evidence during Readiness Review to determine if the security is sufficiently mature to execute an IA certification test event
- Determine the IA test level of effort for each planned System and participate in all test execution and planning activities, including meetings and working groups.

6.2.4. Independent Verification and Validation (IV&V)

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Review DIACAP/RMF documentation prior to IV&V to determine security readiness of system, site, or enclave
- Support the IV&V testing of each system, site, or enclave under the CA and AO purview
- Participate in all test execution and planning activities, including meetings and working groups
- Review all C&A documentation to ensure the information is current,

accurate, and applicable to the article of test

- To support standardization, ensure that all IA test procedures are up to date with all current applicable requirements and that those methods of testing are widely visible and available for CNIC to apply to all necessary systems across its enterprise

- Produce individualized IA test procedures for inclusion in the Test Plan that describe how to perform validation actions as outlined in the applicable STIG checklists

- Analyze previous IA testing artifacts to tailor IA tests

- Develop IV&V Test Plan, provide to system owner, documentation team, and IV&V team

- Oversee the execution of IA certification testing to identify all vulnerabilities, and document residual risks by conducting thorough risk assessments

- Provide the IA risk analysis and mitigation determination results for use in the test report

- Implement/Utilize automated tools, for the creation of necessary test evidence, risk assessment, and certification artifacts for each system

- Perform wireless discovery using DoD software Flying Squirrel and Caribou

- Perform testing with WebInspect

- Perform testing with tools to manage the test procedures and results

- Validator and IV&V Representatives to review DIACAP/RMF documentation prior to IV&V

- Schedule IV&V events and assign IV&V team members to meet the requirements of the IV&V test plan

- Provides status report to the Government PM on progress/results of IA testing

- Identify and elevate the need for any additional IA test events needed to support accreditation (Includes scheduling of annual reviews)

- Coordinate test planning with SMEs identified from IA Validation Team with the CA

6.2.5. Oversight of POA&M and DIACAP/RMF Scorecard creation

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Oversee completion of DIACAP/RMF Scorecard

- Provide Mitigation and Remediation in support of the C&A process both remotely and on-site

- Provide POA&M resolution recommendations to meet DoD and Federal technical and operational requirements and guidelines

- Provide assistance to sites to update outstanding actions contained in the POA&M and requesting extensions for expiring IATOs

6.2.6. Validator

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Maintain qualified validator status with Navy or other applicable DON/CNIC agency requirement

- Review all packages before being delivered to CA

- Work directly with the CA as a qualified agent to ensure validation activities are compliant with the IA test strategy

- Conduct in-depth analysis of IV&V, C&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal IA technical and operational security requirements

- Identify and elevate the need for any additional IA test events needed to support accreditation (Includes scheduling of annual reviews)

- Work with the system owner to create specific site or system mitigation plans to achieve an overall reduction in residual risk

- Coordinates with the CA for issuance of a certification recommendation

6.2.7. Risk Assessments

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

- Provide Mitigation and Remediation in support of the C&A process remotely and/or on-site

- Provide Mitigation and Remediation reports (CDRL A021)

- Conduct in-depth analysis of IV&V, C&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal IA technical and operational security requirements

- Document residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and provide the IA risk analysis and mitigation determination results for the Test Report

- Assist the CA and Validator with producing the risk assessment artifacts describing residual risks identified during certification testing

6.3. Cyber Security Management

6.3.1. C&A Tool Training

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, for the Enterprise Mission Assurance Support Service (eMASS) the contractor shall:

- Provide how-to guides and support efficient use of the eMASS system (CDRL A021)

- Schedule eMASS training for CNIC personnel and provide training documentation (CDRL A021)

- Provide high level eMASS training to new members of Staff

- Assist in the development of the eMASS process flow documents

- Serve as Tier 1 support to address process issues that are identified in eMASS. Elevate and track software issues to DISA through the DISA Enterprise Help Desk.

- Maintain all applicable CNIC Program eMASS user accounts

- Assist CNIC user community with DIACAP/RMF lifecycle for system in eMASS (i.e. System registration, assigning DIACAP/RMF team members, control assessment and validation, uploading artifacts, submitting packages and running applicable reports)

- Establish and manage inheritance for CNIC Enterprise

- Create/run system reports and create organizational metrics to report to leadership team

In compliance with DoD Cybersecurity/IA C&A Directives and Processes, for the Vulnerability Management System (VMS) and Assured Compliance Assessment Solution (ACAS) the contractor shall:

- Provide "How-to-Guides" to support efficient use

- Schedule and perform VMS training for CNIC Personnel and provide training documentation (CDRL A021)

- Schedule and perform ACAS training for CNIC Personnel

- Provide high level training to new staff

- Assist in the development of the VMS Process Flow

- Serve as Tier 1 support to address issues that are identified in VMS. Elevate and track software issues to DISA through the DISA Enterprise Help Desk.

- Assist CNIC user community with DIACAP/RMF lifecycle for system in VMS

(i.e. System registration, assigning DIACAP/RMF team members, control assessment and validation, uploading artifacts, submitting packages and running applicable reports)

- Establish and manage inheritance for CNIC Enterprise

- Create/run system reports and create organizational metrics to report to leadership team

- Maintain all applicable CNIC Program VMS user accounts

6.3.2. Information Assurance System Security Officer (ISSO) Support

The Contractor shall assist the SPAWAR in its responsibility to by investigate, recommend solutions and remediating issues associated with systems, applications and data centers for Security Authorization packages to achieve Authority to Operate (ATO). The CNIC N6 currently has a Portfolio of 133 systems for which they have direct ISSO responsibility. Some are located on the CESCs, PSNet and various legacy network enclaves at various CNIC locations. Additionally, the contractor will provide ongoing Post-ATO POA&M tracking and remediation and support for authorized security scans/audits/assessments. The Contractor shall also:

- Complete and maintain all Defense Information Assurance Certification and Accreditation Program (DIACAP) or Risk Management Framework (RMF) documentation packages,

- Update these document packages at least annually or as the system changes,

- Complete and maintain Interconnection Agreements (ICAs) for any connections external to CNIC N6 management,

- Maintain applicable repository of any related Memorandum of Agreement/Understanding (MOA/MOU) or copies of these agreements if they are applicable to cybersecurity management,

- Ensure all Committee on National Security Systems (CNSS) SCs and requirements are met at inception and throughout system lifecycle

- Ensure that security requirements are being or will be met to obtain/maintain a valid ATO status,

- Ensure system is properly patched and hardened according to DoD and DON requirements,

- Ensure all IS privilege users have valid signed Navy System Authorization Access Request (SAAR-N) and privilege access forms on file,

- Ensure that weaknesses are identified, documented, addressed and remediated through the POA&M tracking process, waivers and/or exceptions,

- Complete Waivers, Exceptions and Accepted Risks (WEAR) and to meet CNIC operational standards and requirements,

· Complete a remediation plan for all opened POA&Ms entries for the ATO brief,

· Provide code review & approval prior to deployment into production,

· Review audit logs on a weekly basis,

· Ensure visitor log at CESCs in Norfolk, VA and San Diego, CA and PSNet Network Operations Center (NOC) in Alexandria, VA are being utilized and maintained for access to system components and review the visitor logs on at least monthly,

· Review monthly scan reports and open POA&Ms,

· Conduct Annual Assessments and Testing by CNIC,

· Ensure maintenance of system components is implemented via the Change, Configuration and Release Management (CCRM) processes and procedures,

· Report IT security incidents (including computer viruses and malwares) in accordance with established procedures, including the incident response process and procedures,

· Report security incidents not involving IT resources to the appropriate security office,

· Ensure that requests for A&A of ISs are completed in accordance with the defined procedures,

· Ensure compliance with all legal requirements concerning the use of commercial proprietary software, e.g. respecting copyrights and obtaining site licenses,

· Ensure that risk analyses are completed to determine cost-effective and essential safeguards,

· Attend security awareness and related training programs and distributing security awareness information to the user community as appropriate,

· Provide input to appropriate IT security personnel for preparation of reports to higher authorities concerning sensitive and/or national security ISs,

· Support the development of contingency plans, disaster recovery (DR) plans, and Continuity of Operations (COOP) testing, and failover testing consisting of documented contingency plans,

· Provide consultation in the development of Contingency and Disaster recovery plans for CNIC ISs and their operations,

· Determine and document how IT capability will be maintained during an emergency (e.g., fire, flood, power outage, interruption of telecommunications service, or other possible emergency situations),

· Work with a third party contractor in assisting in the development of the COOP plan,

- Participate in the annual COOP exercises and DR?tests. COOP and DR tests are required for each system over which CNIC N6 has ISSO responsibility, and

- Assist CNIC Code N6C by investigating, recommending solution and remediating issues associated with systems, applications and data centers for an A&A package to achieve ATO.

6.3.3. Certification and Accreditation (C&A) Documentation Support

- Develop all C&A documentation in accordance with DoD policies, CNIC policies and procedures to ensure that accreditation packages are complete and system compliance is met for Navy Authorizing Official

- Maintain documentation Plan of Action and Milestones

- Develop C&A documentation to ensure the information is current, accurate, and applicable to the article of test

- Develop IA self-assessment results and evidence during Information Assurance Validation Readiness Review (IAVRR) to determine if the system security is sufficiently mature to execute the IA certification test event

- Participate in DIACAP / RMF Team Meetings

- Utilize Enterprise Mission Assurance Support Services (eMASS) and the Vulnerability Management System (VMS) for the documentation of test evidence and risk assessment for each system

- Develop required artifacts and provide security control implementation information for C&A Packages

- Develop associated DIACAP / RMF IA Artifacts to include the System Security Plan, System Design and Architecture, Contingency Plan/COOP Plan, Incident Response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote Access artifacts

6.3.4. Information Assurance Self Assessments and Cybersecurity Inspection and Certification Program (CISCP) Phase II Cybersecurity Inspections

Preparations:

- Work with IV&V Lead from CNIC to develop Test Plan

- Participate in System related meetings

- Prepare for onsite self-assessment and/or CSICP Phase II inspection

Self-Assessment Execution:

- Execute tests per the Test Plan

- Prepare test events status reports and outbriefs (CDRL A021)
- Populate Validator database/VMS/eMASS with test results
- Contribute to Test Event Reporting
- Assemble DIACAP / RMF Package (DIACAP / RMF Scorecard, Plans of Action & Milestones (POA&M), Certification Documentation, and System-provided System Identification Profiles (SIP) & DIACAP / RMF Implementation Plans)
- Develop plans to validation actions as outlined in the applicable Security Technical Implementation Guide (STIG) checklists
- Validate DIACAP / RMF Implementation Plan (DIP)
- Assist IA Analyst / Test Team Lead with evaluating IA self-assessment results and evidence
- Participate in DIACAP / RMF Team Meetings
- Ensure IA test procedures are available and visible for use of replication across System using the same software
- Utilize eMASS and VMS for the documentation of test evidence and risk assessment for each System

Create Policy and Provide Policy Guidance

- Develop/maintain agency level cybersecurity policy and processes that implements DoD Cybersecurity program
- Develop/maintain agency level cybersecurity policies and processes
- Develop/maintain agency level RMF policy
- Provide training, reporting, guidance and support to meet the requirements of the DoD IA Workforce Improvement Program Provide guidance on recommended contracting language for built in security for IT solutions (CDRL A021)
- Ensures enterprise-wide compliance reporting is standardized across CNIC and meets DoD cybersecurity policy requirements

IT Exercise and Contingency Planning

- Provide guidance and support related IT contingency planning (ITCP)
- Develop templates in support of ITCP
- Develop and maintain procedures related to tabletop exercises for contingency plans, as well as develop scenarios
- Support execution of tabletop exercises for CNIC community
- Participating in the tabletop exercise

- Provide summary of scenario outcomes and recommended changes to specific ITCP plan being reviewed

Cybersecurity Workforce (CSWF) Report

CSWF Reports (CDRL A003) shall be developed, maintained, and submitted monthly at the contract or task order level. If Information Assurance (IA) support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified

Asset, Configuration and Change Management

Asset Management (CDRL A011)

- CNIC N6 requires support for the physical and electronic receipt, inventory, and transfer of cybersecurity related hardware, software, appliances, equipment and resources. The Contractor shall actively manage all assets of cybersecurity related hardware, software, appliances and system, including:

- Maintenance of asset database to the extent that inventory updates of newly installed or moved systems are input,

- Maintenance of configuration,

- Management of receiving of new assets, shipment of assets and their location, deployment status,

- Disposition of N6 approved hardware, software, appliances, equipment and resources, including data destruction of the sensitive data on CNIC IT equipment to be disposed in accordance with N6 approved data deposition process,

- Yearly audit of cybersecurity operational inventory with Code N6 supervision

- Projection of annual recurring costs for software license and support service renewal, and

- Recommendation of new assets requirements, and

- Preparation of asset reports based on inventory data, projection and recommendations.

Configuration Management

- The Contractor shall actively manage configuration of all assets of cybersecurity managed related hardware, software, appliances and system. Configuration Management (CM) provides governance to establish and maintain the integrity of asset Configuration Items (CIs), such as IT service software, assets, products, devices, and documentation, throughout the CI lifecycle. CM provides governance over the procedures by which tasks can effectively manage, modify, and version these service asset CIs in order to create and maintain an accurate baseline. This baseline is the foundation for lifecycle management and provides the ability to recreate a service asset instance in the event that a rollback is required or if the recreation of a system is necessary due to a catastrophic loss. The Contractor shall conduct the following CM activities:

· Administer the CNIC cybersecurity management related CM program in accordance with established CM policy,

· Provide the daily management and oversight of the CM tools,

· Establish and document Operations and Maintenance procedures for the CM tools, (CDRL A021)

· Maintain applicable items in the N6 electronic document library for cybersecurity assets,

· Review all cybersecurity CM related documentation and provide valuable comments/feedback,

· Participate in all CM related ad hoc meeting requests,

· Maintain an accurate accounting of all configuration items that are associated with CNIC cybersecurity,

· Recommend and document configuration identification standards for software, hardware, and documentation CIs,

· Conduct a review of the system CIs for each release to ensure systems comply with the establishment of a baseline (CDRL A021) for each release, and

· Conduct configuration audits and accounting at least annually.

Change Management

· The Contractor shall conduct the following Change Management activities:

· Administer the CNIC cybersecurity related Change Management program in accordance with established policy,

· Provide project support and have knowledge of the CNIC Code N6 Change Control Processes,

· Assist in review and impact assessment of various cybersecurity related Change Requests (CRs) as necessary,

· Update change policy to support lean and service oriented change practices, and

· Continuously evaluate external and internal policies and practices to reduce unessential practices.

6.4. Program Management Support

6.4.1. The contractor shall provide program management support. Support includes:

- Program and task order specific metrics reporting in various sponsor and task formats
- Program and task order specific financial reporting in various sponsor and task formats (CDRL A002)
- Provide Inventory Tracking Report as part of (CDRL A011)
- Provide Contract Funds Status Report (CFSR) (CDRL A018)
- Provide WAWF Invoicing Notification and Support Documentation (CDRL A016)
- Provide Quality Documentation (CDRL A007)
- Provide status report to the Government PM on progress/results of IA testing
- Support and provide minutes and status reports for collaborative meetings
- Providing Information Assurance oversight, project management, and logistics for the task
- Provide project management, planning, and coordination support
- Work with Integrated Product Team (IPT) to ensure project management and reporting templates are defined and maintained for all new drafts
- Develop tools utilizing capabilities such as: Microsoft SharePoint, Access, or Excel

7.0 GOVERNMENT FURNISHED INFORMATION (GFI)

No GFI will be provided on this TO

8.0 GOVERNMENT FURNISHED PROPERTY (GFP)

8.1 GOVERNMENT FURNISHED EQUIPMENT (GFE)

No GFE will be provided on this TO

8.2 GOVERNMENT FURNISHED MATERIAL (GFM)

No GFM will be provided on this TO

9.0 CONTRACTOR ACQUIRED PROPERTY (CAP)

9.1 CONTRACTOR ACQUIRED EQUIPMENT (CAE)

No CAE is allowed on this TO

9.2 CONTRACTOR ACQUIRED MATERIAL (CAM)

No CAM is allowed on this TO

10.0 TRAVEL

Extensive travel may be required in support of this task order. The following locations are travel requirements:

For estimating purposes, it is anticipated that the following travel requirements may be necessary:

# Trips	# People	# Days/Nights	From (Location)	To (Location)
9	2	5	Charleston, SC	Washington, DC
12	2	5	Charleston, SC	Norfolk, VA
12	7	5	Washington, DC	Norfolk, VA
9	7	5	Washington, DC	Charleston, SC
3	2	5	Norfolk, VA	Charleston, SC
6	2	5	Norfolk, VA	Washington, DC
6	2	5	San Diego, CA	Washington, DC
9	2	5	Charleston, SC	San Diego, CA
3	2	5	Norfolk, VA	San Diego, CA

11.0 TRANSPORTATION OF EQUIPMENT/MATERIAL

No transportation of equipment/material is required on this TO

12.0 DELIVERABLES

12.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

12.1.1 Administrative CDRL

As required under TO PWS 6.1 - 6.30 the following table lists all required administrative data deliverables, Contract Data Requirements Lists (CDRLs), applicable to this task:

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
A016	Invoice Support Documentation	6.3.4	As Needed	30 Days after task order (DATO) and monthly on the 10th
A002	Task Order Status Report	6.1-6.3	As Needed	Within 24 hours from request
A004	Contractor Manpower Quarterly Status Report	6.1-6.3	QRTLY	30 DATO and on the 10th
A005	Task Order Close Out Report	6.1-6.3	As Needed	NLT 10 DATO
A006	Contractor Census Report	6.1-6.3	MTHLY	30 Days after task order (DATO) and monthly on the 10th
A008	Cost and Schedule Milestone Plan	6.1-6.3	As Needed	30 Days after task order (DATO) and monthly on the 10th
A009	Contractor CPARS Draft Approval Document (CDAD) Report	6.1-6.3	As Needed	30 Days after Contract Award
A003	Cyber Security Workforce (CSWF) Report	6.3.4	As Needed	30 Days after Contract Award

12.1.2 Technical CDRL

The following table lists all required technical data deliverables, Contract Data Requirements Lists (CDRLs), applicable to this task:

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
A021	Technical/Analysis Reports, General	6.1.6, 6.1.7, 6.1.9, 6.1.10, 6.2.7, 6.3.1, 6.3.4	As Needed/Monthly /Weekly	As Required
A007	Quality Documentation	6.4.1	As Needed	24 hrs after Request
A011	Inventory Tracking Report	6.3.4, 6.4.1	Monthly	30 Days after task order (DATO) and

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
				monthly on the 10th
A018	Contract Funds Status Report (CFSR)	6.4.1	Monthly	30 Days after task order (DATO) and monthly on the 10th

12.2 NON-DATA DELIVERABLES N/A

13.0 SUBCONTRACTING REQUIREMENTS

Subcontracting requirements are in accordance with the basic contract. Note: If a prime contractor plans to utilize subcontractor(s) on this Task Order, the prime must specify in their proposal the intent to utilize subcontractors and list all applicable subcontractor names. Per clause 52.244-2, if a subcontractor is proposed by a prime and is not approved on the basic contract, formal justification is required and subject to government approval.

14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP), Attachment 5 of the RFP.

15.0 OTHER CONDITIONS/REQUIREMENTS

15.1 TO SUPPLEMENTAL PERSONNEL QUALIFICATION

The contractor shall have the following certifications: It is the responsibility of the contractor to have these positions staffed with these certifications within six (6) months of initial award. The Government considers these certifications/qualifications to be essential to the performance of this Task Order.

- Certification: CompTIA Advanced Security Practitioner (CASP)
- Certification: Certified Information Systems Security Professional (CISSP)
- Certification: Certified Cisco Network Administrator (CCNA)

o Qualification: DoD Information Assurance Technician (IAT) Level III or IA System Administrator/Engineer (IASAE) Level II (Multiple Positions)

o Qualification: Qualify as a DoD Computer Network Defense (CND) Analyst. (Multiple Positions)

- Certification: Certified ForeScout Engineer and CISSP or CASP (One Position)

- Certification: Fully Qualified Navy Validator (Multiple positions)

o Qualification: Name must be published on the US Fleet Cyber Commands list of Fully Qualified Navy Validators (FQNV)

16.0 LIST OF ATTACHMENTS

Attachment 5 of the RFP – Quality Assurance Surveillance Plan (QASP)

SECTION D PACKAGING AND MARKING

All Deliverables shall be packaged and marked IAW Best Commercial Practice.

SECTION E INSPECTION AND ACCEPTANCE

CLIN	INSPECT AT	INSPECT BY	ACCEPT BY	ACCEPT BY
2001	Destination	Government	Destination	Government
3001	Destination	Government	Destination	Government
4001	Destination	Government	Destination	Government

SECTION F DELIVERABLES OR PERFORMANCE

The periods of performance for the following Items are as follows:

2001	12/23/2015 - 12/22/2016

CLIN - DELIVERIES OR PERFORMANCE

The periods of performance for the following Items are as follows:

2001 Date of Contract Award - 365 Days after contract award

3001 Begins after CLIN 2001 is complete and ends 365 days after CLIN 3001 is exercised

4001 Begins after CLIN 3001 is complete and ends 365 days after CLIN 4001 is exercised

SECTION G CONTRACT ADMINISTRATION DATA

(b)(6)
SSC Lant
(b)(6)@navy.mil
843-218-(b)(6)

The SPAWAR Atlantic Ombudsman is Steven G. Harnig, (843) 218-4560.

THIS IS A COST PLUS FIXED FEE, LEVEL OF EFFORT TYPE ORDER.

The number of hours estimated for this LOE tasking is based on one (1) twelve (12) month base year and two (2) one-year option periods. **The total estimated labor hours is 175,580 standard hours (per year) and no overtime hours (totaling 526,740 for all years).** In performing the requirements of this order, the contractor may use any combination of hours from the labor categories approved at the basic contract level, so long as the estimated total cost and the funded amount to date for the order is not exceeded and the total number of hours provided does not exceed the estimated number of hours by more than 5%.

5252.232.9400 LIMITATION OF LIABILITY- INCREMENTAL FUNDING (JAN 1992)

This TASK order is incrementally funded and the amount currently available for payment hereunder is limited to $100,000 inclusive of fee. It is estimated that these funds will cover the cost of performance through 9/30/2016. Subject to the provision of the clause entitled Limitation of Funds (FAR 52.232-22) of the general provisions of this contract, no legal liability on the part of the Government for payment in excess of $100,000 shall arise unless additional funds are made available and are incorporated as a modification to the TASK order.

Estimated CPFF Total Order NTE*	Total Funded Amount	Unfunded Amount
$11,389,044.55	$100,000.00	$11,289,044.55

The contractor shall cite on each invoice/voucher, in addition to all other requirements of this contract/order, the contract line item number (CLIN); the contract subline item number (SLIN) and accounting classification reference number (ACRN) for the portion, or portions of work being billed as specified in the contract or delivery order. For each ACRN on the invoice/voucher, the contractor shall identify the amount being billed against that ACRN.

252.232-7006 Wide Area WorkFlow Payment Instructions.

(a) *Definitions.* As used in this clause—

"Department of Defense Activity Address Code (DoDAAC)" is a six position code that uniquely identifies a unit, activity, or organization.

"Document type" means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF). "Local processing office (LPO)" is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) *Electronic invoicing.* The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) *WAWF access.* To access WAWF, the Contractor shall—

(1) Have a designated electronic business point of contact in the System for Award Management at https://www.acquisition.gov; and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this web site.

(d) *WAWF training.* The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at https://wawf.eb.mil/

(e) *WAWF methods of document submission.* Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) *WAWF payment instructions.* The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) *Document type.* The Contractor shall use the following document type(s).

Cost Type Orders - Cost Voucher

(2) *Inspection/acceptance location.* The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

N65236

(3) *Document routing.* The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table

*Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	DFAS (HQ0338)
Issue By DoDAAC	N65236
Admin DoDAAC	DCMA Baltimore (S2101A)
Inspect By DoDAAC	N65236
Ship To Code	N65236
Ship From Code	N/A
Mark For Code	N65236
Service Approver (DoDAAC)	DCMA Baltimore (S2101A)
Service Acceptor (DoDAAC)	N/A
Accept at Other DoDAAC	N/A
LPO DoDAAC*****	
DCAA Auditor DoDAAC	HAA210
Other DoDAAC(s)	N/A

	Cost Type Orders	Fixed Price Orders
WAWF Invoice Type	Cost Voucher	2-N-1 (Services Only)
Issuing Office DODAAC	N65236	N65236
Admin DODAAC:	DCMA (S2101A)	DCMA (S2101A)
Inspector DODAAC (if applicable)	N65236	N65236
Acceptor DODAAC:	N65236	N65236
LPO DODAAC:	N65236	N65236
DCAA Auditor DoDAAC:	DCAA (HAA210)	DCAA (HAA210)
Service Approver DoDAAC:	DCMA (S2101A)	DCMA (2101A)
PAY DODAAC:	DFAS HQ0338	DFAS HQ0338

(4) *Payment request and supporting documentation.* The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (*e.g.* timesheets) in support of each payment request.

(5) *WAWF email notifications.* The Contractor shall enter the e-mail address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.

(b)(6)
SSC Lant
(b)(6)@navy.mil
843-218-(b)(6)

(g) *WAWF point of contact.*

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

(b)(6)
SSC Lant
(b)(6)@navy.mil
843-218-(b)(6)

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

252.204-0002 Line Item Specific: Sequential ACRN Order. (SEP 2009)

The payment office shall make payment in sequential ACRN order within the line item, exhausting all funds in the previous ACRN before paying from the next ACRN using the following sequential order: Alpha/Alpha; Alpha/numeric; numeric/alpha; and numeric/numeric.

```
Accounting Data

SLINID   PR Number                                           Amount
-------- --------------------------------------------------  --------------------
200101   130053983300001                                     100000.00
LLA :
AA 1761804 52FA 251 00052 0 068732 2D C001SC 000526ITQ14Q
Standard Number: N6523615PR02941
ACRN: AA
COST CODE: 000526ITQ14Q
PLANNING PR #: 1300486765
FUNDED PR#: 1300539833
CRM #: 15-00757
Standard Doc. #: N6523615PR02941
Funding Doc #: N0005216RC001SC


BASE Funding 100000.00
Cumulative Funding 100000.00
```

SECTION H SPECIAL CONTRACT REQUIREMENTS

DISTRIBUTION

Contractor Cage 15151 Honeywell Technology Solutions, Inc. 7000 Columbia Gateway Drive Columbia, MD 21046-2119 **Local Office:** Honeywell Technology Solutions, Inc. 5935 Rivers Avenue, Suite 100 North Charleston, SC 29406 POC: Jerry Erar Principal Contracts Manager (840) 300-4782 Gerald.Erar@Honeywell.com	**DCAA Baltimore Branch Office HAA210** 8140 Corporate Drive Suite 100 Baltimore, MD 21236 POC: Luise Fortney, Supervisory Auditor (410) 964-7684 Luise.fortney@dcaa.mil
DCMA Baltimore Branch Office S2101A 217 East Redwood Street Suite 1800 Baltimore, MD 21202-3375 POC: Mr. Glenn Schildgen, Divisional Administrative Contracting Officer (410) 962-9490 Glenn.schildgen@dcma.mil	**COR** (b)(6) **Contract Specialist** Melissa (Lisa) A. Connell, 2221LC Lisa.connell@navy.mil (843) 218-2701
DFAS Columbus Center HQ0338 DFAS-CO/South Entitlement Operations P.O. Box 182264 Columbus, OH 43218-2264 POC: Mary Ellen Duffy 800-756-4571, ext. 12 dfas_columbus@dfas.mil	